

IZDAVANJE DIGITALNIH SERTIFIKATA SERTIFIKACIONOG TELA POŠTE

Dragan Spasić
Javno preduzeće PTT saobraćaja "Srbija"

Sadržaj: *U radu je objašnjen postupak izdavanja digitalnih sertifikata Sertifikacionog tela Pošte pravnim i fizičkim licima.*

Ključne reči: *Sertifikaciono telo - CA, digitalni sertifikati, Zakon o elektronskom potpisu.*

1. Uvod

Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je izgradilo Sertifikaciono telo Pošte u skladu sa Zakonom o elektronskom potpisu ("Službeni glasnik Republike Srbije", broj 135, 21.12.2004. godine) i podzakonskim aktima ("Sl. glasnik RS", br. 48/2005). Sertifikaciono telo Pošte izdaje zainteresovanim korisnicima, koji mogu da budu pravna i fizička lica, sledeće četiri (4) kategorije digitalnih (elektronskih) sertifikata [1, 2]:

1. **WEB sertifikate**,
2. **SID Enterprise sertifikate** (Single application ID),
3. **MID Enterprise sertifikate** (Multiple application ID),
4. **SER sertifikate za Web servere**.

Digitalni sertifikati Sertifikacionog tela Pošte su standardni X.509 verzija 3 sertifikati koji mogu da se koriste za autentifikaciju (predstavljanje) Web korisnika i Web servera, šifrovanje / dešifrovanje i digitalno potpisivanje / verifikovanje potpisanih datoteka, elektronskih pisama i transakcija, u okviru aplikacija koje podržavaju rad sa digitalnim sertifikatima.

U ovom trenutku (oktobar 2006.), PTT tj. Sertifikaciono telo Pošte je prvo i jedino **javno** sertifikaciono telo u Republici Srbiji. Primarni cilj PTT-a kao sertifikacionog tela je da se registruje za izdavanje KVALIFIKOVANIH digitalnih

sertifikata u Republici Srbiji, i time dobije licencu za izdavanje KVALIFIKOVANIH digitalnih sertifikata. Nadležan organ za registrovanje sertifikacionih tela u Republici Srbiji je Ministarstvo za nauku i zaštitu životne sredine, u okviru koga postoji Sektor za informaciono društvo.

Implementacija Zakona o elektronskom potpisu (br. 135/2004) je nekoliko puta odlagana (1.9.2005., 1.1.2006., 1.7.2006.). Konačno, implementacija Zakona je počela **1.7.2006.** PTT je **18.7.2006.** dostavio Ministarstvu nauke i zaštite životne sredine: "Zahtev za upis u registar sertifikacionih tela za izdavanje KVALIFIKOVANIH elektronskih sertifikata u Republici Srbiji", "Prijavu za upis u evidenciju sertifikacionih tela" i prateću dokumentaciju, tako da PTT očekuje da u najskorije vreme Sertifikaciono telo Pošte bude registrovano za izdavanje KVALIFIKOVANIH digitalnih sertifikata u Republici Srbiji.

Prema nacrtu Strategije razvoja poštanskog saobraćaja u Republici Srbiji do kraja 2010. godine, napisane u leto 2006. godine, jedan od strateških ciljeva je da javni poštanski operater dobije ulogu nacionalnog sertifikacionog tela imajući u vidu opšti interes države.

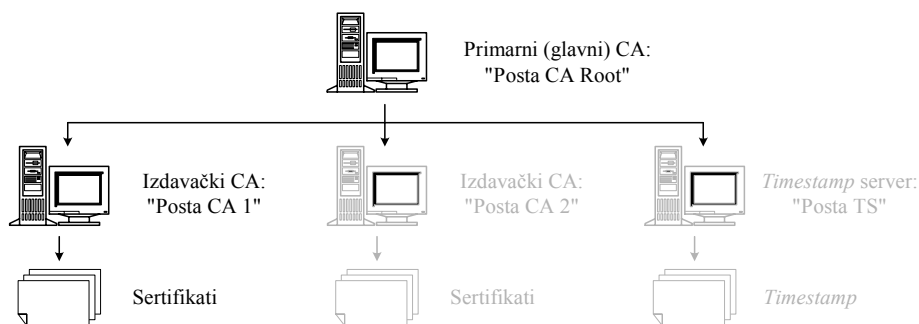
2. Hijerarhijska organizacija Sertifikacionog tela Pošte

Sertifikaciono telo Pošte koristi u svojoj infrastrukturi za izdavanje X.509 verzija 3 digitalnih (elektronskih) sertifikata, hijerarhiju više CA (Certification Authority) servera koji se nalaze u relaciji nadređeni-podređeni CA serveri. Infrastrukturu Sertifikacionog tela Pošte u ovom trenutku čine dva CA servera (slika 1. i 2.):

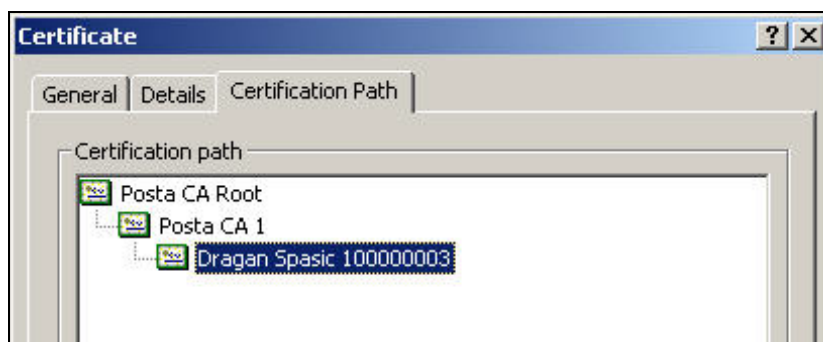
- "Posta CA Root" server, kao primarno (glavno) tj. **ROOT** sertifikaciono telo.
- "Posta CA 1" izdavački server, kao podređeno sertifikaciono telo.

Planirano je da se naknadno instaliraju (slika 1.):

- Dodatni izdavački CA server "Posta CA 2".
- *Timestamp* server "Posta TS".



Slika 1. Hijerarhijska organizacija CA servera Sertifikacionog tela Pošte



Slika 2. Sertifikaciona putanja sertifikata Sertifikacionog tela Pošte

3. Postupak izdavanja digitalnih sertifikata korisnicima

Postupak izdavanja digitalnih sertifikata korisnicima se sastoji od nekoliko koraka (slika 3.) [1, 2]:

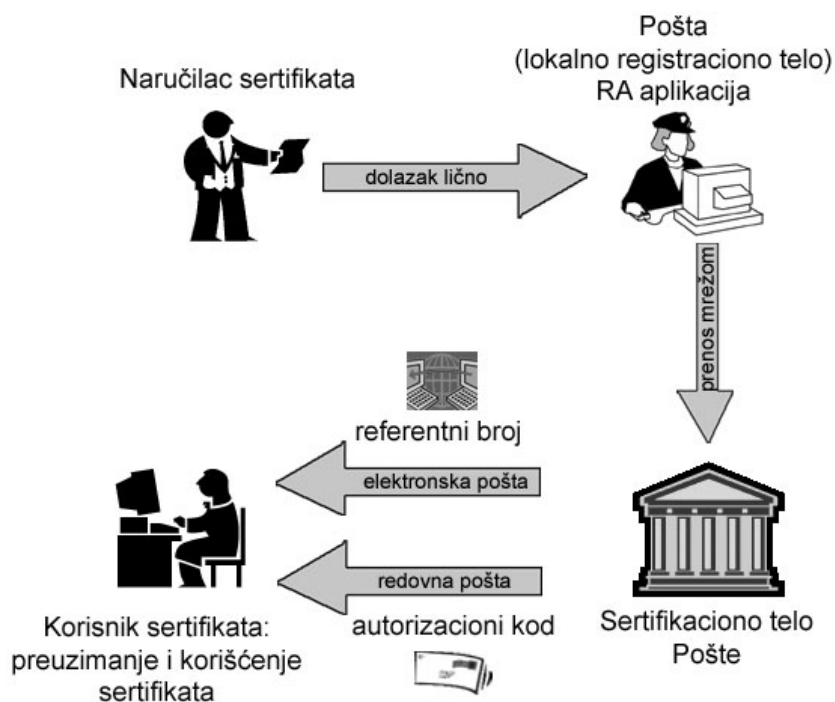
1. Naručilac, odnosno ovlašćeno lice koje učestvuje u postupku izdavanja sertifikata, u bilo kojoj pošti (lokalno registraciono telo) koja je ovlašćena za prihvatanje zahteva za izdavanje sertifikata, šalterskom radniku predaje:
 - popunjen i potpisan Ugovor o izdavanju i korišćenju elektronskog sertifikata za fizičko lice / pravno lice [3, 4],
 - prateću dokumentaciju za fizičko lice / pravno lice (videti poglavlje 4. i 5.),
 - overeni prvi primerak uplatnice ("Nalog za uplatu"; videti poglavlje 6.) koja predstavlja potvrdu da je izvršena uplata prema Cenovniku (<http://www.cepp.co.yu/ca/cenovnik>).
2. Šalterski radnik u pošti utvrđuje identitet naručioca, odnosno ovlašćenog lica na osnovu lične karte ili pasoša i proverava podatke koje je naručilac, odnosno ovlašćeno lice upisalo na Ugovoru i uplatnici ("Nalog za uplatu"), kao i predatu prateću dokumentaciju.
3. Šalterski radnik vrši unos prikupljenih podataka korišćenjem RA aplikacije, čime se vrši upis korisnika u bazu korisnika Sertifikacionog tela Pošte.
4. Sertifikaciono telo Pošte dostavlja korisniku dva podatka za preuzimanje sertifikata:
 1. **referentni broj** (Reference number) elektronskom poštom (E-mail) i 2. **autorizacioni kod** (Authorization code) redovnom poštom na adresu naznačenu u Ugovoru [3, 4]. Ukoliko korisnik ne poseduje adresu elektronske pošte, i **referentni broj** i **autorizacioni kod** će mu biti dostavljeni poštom na adresu naznačenu u Ugovoru. U slučaju izdavanja sertifikata na smart kartici, korisnik će biti obavešten da preuzme smart karticu sa sertifikatom u određenoj pošti ili će mu smart kartica biti dostavljena poštom na adresu naznačenu u Ugovoru.
5. Korisnik preuzima sertifikat na osnovu **referentnog broja** i **autorizacionog koda**:
 - WEB sertifikati se preuzimaju korišćenjem Web pretraživača **Microsoft Internet Explorer** 5.0 ili novijim (Cipher Strength: 128-bit), u skladu sa korisničkim uputstvom "**Preuzimanje Web sertifikata**" [5].

- SID i MID Enterprise sertifikati se preuzimaju korišćenjem korisničke aplikacije **Entrust Entelligence**, u skladu sa korisničkim uputstvom "**Preuzimanje Entrust Enterprise sertifikata**" [6].

U slučaju da je naručilac sertifikata pravno lice, moguće je da ovlašćeno lice pravnog lica popunjen i potpisan Ugovor [4] i prateću dokumentaciju za pravno lice preda ovlašćenom licu u Sertifikacionom telu Pošte, umesto šalterskom radniku u pošti (lokalno registraciono telo) koja je ovlašćena za prihvatanje zahteva za izdavanje sertifikata. Tada je moguće da pravno lice izvrši plaćanje usluge izdavanja i korišćenja sertifikata prema fakturi dostavljenoj od Sertifikacionog tela Pošte.

Osim digitalnih sertifikata, naručilac, odnosno ovlašćeno lice može da podnese zahtev za kupovinu i Entrust aplikacionih dodataka tj. *plug-in*-ova **Entrust ICE** i **Entrust Express**.

U ovom trenutku, jedina operacija za promenu statusa sertifikata koju Sertifikaciono telo Pošte naplaćuje je produženje korišćenja sertifikata za željeni broj godina [7, 8].



Slika 3. Postupak izdavanja digitalnih sertifikata korisnicima

4. Prateća dokumentacija za fizičko lice

Fizičko lice ili lice ovlašćeno od strane fizičkog lica za učestvovanje u postupku izdavanja sertifikata, dužno je da šalterskom radniku preda:

1. Fotokopiju ličnog dokumenta fizičkog lica kojem se izdaje sertifikat (prve četiri strane lične karte ili prve dve strane pasoša).
2. Dokument, odnosno fotokopiju dokumenta, kojim lice koje se pojavljuje pred šalterskim radnikom dokazuje da je ovlašćeno za učestvovanje u postupku izdavanja sertifikata i to:
 - 2.1. ako je ovlašćeno lice roditelj - izvod iz matične knjige rođenih,
 - 2.2. ako je ovlašćeno lice staralac - rešenje kojim ga je nadležni državni organ proglasio za staraoca,
 - 2.3. ako je ovlašćeno lice advokat - sudski overeno punomoćje.
3. Fotokopiju ličnog dokumenta ovlašćenog lica (prve četiri strane lične karte ili prve dve strane pasoša).

5. Prateća dokumentacija za pravno lice

Odgovorno lice pravnog lica ili lice ovlašćeno od strane pravnog lica za učestvovanje u postupku izdavanja sertifikata, dužno je da šalterskom radniku preda:

1. Fotokopiju izvoda iz registra nadležnog organa u koji je upisan naziv, matični broj i PIB (poreski identifikacioni broj) pravnog lica.
2. Dokument, odnosno fotokopiju dokumenta, kojim lice koje se pojavljuje pred šalterskim radnikom dokazuje da je ovlašćeno za učestvovanje u postupku izdavanja sertifikata i to:
 - 2.1. ako je ovlašćeno lice odgovorno lice pravnog lica - izvod iz registra u kojem je upisano kao odgovorno lice,
 - 2.2. ako je ovlašćeno lice zaposleni u pravnom licu - potvrdu tj. ovlašćenje izdato od strane odgovornog lica pravnog lica da je ovlašćeno od istog za učestvovanje u postupku izdavanja sertifikata i da je zaposleno u tom pravnom licu,
 - 2.3. ako je ovlašćeno lice advokat - sudski overeno punomoćje.
3. Fotokopije ličnih dokumenata ovlašćenog lica i korisnika za koje pravno lice naručuje sertifikat/e (prve četiri strane lične karte ili prve dve strane pasoša).

6. Uplatnica "Nalog za uplatu"

Naručilac, odnosno ovlašćeno lice može da izvrši uplatu prema Cenovniku na istom šalteru na kojem se registruje zahtev za izdavanje sertifikata, na drugom šalteru iste pošte, na šalteru u drugoj pošti ili na šalterima drugih učesnika u platnom prometu (banaka).

Naručilac, odnosno ovlašćeno lice dužno je da popuni sledeća polja uplatnice ("Nalog za uplatu") koja je prikazana na slici 4.:

- uplatilac: naziv uplatioca, pravnog ili fizičkog lica i adresa uplatioca

- svrha uplate: izdavanje sertifikata Sertifikacionog tela Pošte, produženje korišćenja sertifikata Sertifikacionog tela Pošte, kupovina *plug-in*-a Sertifikacionog tela Pošte ili drugo
- primalac: RJ za elektronsko poslovanje - CePP, Katićeva 14-18, 11000 Beograd
- šifra plaćanja: 189
- valuta: DIN
- iznos: iznos u dinarima, prema Cenovniku (napomena: numerički podatak iznosa upisuje se sa parama u dve decimale, i to tako što se dinari odvajaju zarezom)
- račun primaoca: 200-2210900101000-05
- model ili broj modela: 97
- poziv na broj (odobrenje): 33102292

Prvi primerak overene uplatnice ("Nalog za uplatu") ostaje šalterskom radniku u pošti prilikom zaključenja Ugovora, odnosno prilikom podnošenja Zahteva za produženje korišćenja sertifikata.

НАЛОГ ЗА УПЛАТУ	
уплатилац	шифра плаћања
	валута
	износ
сврха уплате	рачун примаоца
примаоца	модел и позив на број (одобрење)
печат и потпис уплатиоца	датум валуте
место и датум пријема	

Образац бр. 1

Slika 4. "Nalog za uplatu"

7. Dokumentacija

Dokumentacija koja je namenjena korisnicima usluga Sertifikacionog tela Pošte, dostupna je na Web strani: <http://www.cepp.co.yu/ca/dokumentacija>. Dokumentacija je svrstana u četiri (4) kategorije tj. tabele:

1. Zakoni i podzakonska akta (tabela 1.).
2. Javna dokumenta Sertifikacionog tela Pošte (tabela 2.).
3. Ugovori i Zahtevi Sertifikacionog tela Pošte (tabela 3.).
4. Korisnička uputstva Sertifikacionog tela Pošte (tabela 4.).

Tabela 1. *Zakoni i podzakonska akta*

RB	Naslov dokumenta
1	Zakon o elektronskom potpisu. Zakon je objavljen u "Službenom glasniku Republike Srbije", broj 135, 21.12.2004. godine.
2	Pravilnik o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa ("Sl. glasnik RS", br. 48/2005)
3	Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata ("Sl. glasnik RS", br. 48/2005)
4	Pravilnik o registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji ("Sl. glasnik RS", br. 48/2005)
5	Pravilnik o evidenciji sertifikacionih tela ("Sl. glasnik RS", br. 48/2005)

Tabela 2. *Javna dokumenta Sertifikacionog tela Pošte*

RB	Naslov dokumenta
1	Pravilnik o elektronskim sertifikatima Javnog preduzeća PTT saobraćaja "Srbija" (Certification Practice Statement - CPS). Pravilnik je objavljen u "Službenom PTT glasniku", broj 341, 8.10.2004. godine.
2	Izjava o delatnosti Javnog preduzeća PTT saobraćaja "Srbija" kao sertifikacionog tela (PKI Disclosure Statement - PDS)

Tabela 3. *Ugovori i Zahtevi Sertifikacionog tela Pošte*

RB	Naslov dokumenta
1	Ugovor o izdavanju i korišćenju elektronskog sertifikata za fizičko lice
2	Ugovor o izdavanju i korišćenju elektronskog sertifikata za pravno lice i Prilog
3	Zahtev za izdavanje i korišćenje elektronskog sertifikata i Prilog (napomena: važi samo za zaposlene u JP PTT saobraćaja "Srbija")
4	Zahtev za promenu statusa elektronskog sertifikata fizičkog lica
5	Zahtev za promenu statusa elektronskog sertifikata pravnog lica

Tabela 4. *Korisnička uputstva Sertifikacionog tela Pošte*

RB	Naslov dokumenta
1	Hardverski i softverski preduslovi za instalisanje Entrust klijentskih aplikacija i instalisanje i uklanjanje Entrust klijentskih aplikacija
2	Preuzimanje Entrust Enterprise sertifikata
3	Obnova Entrust Enterprise profila korisnika
4	Potpisivanje i šifrovanje datoteka korišćenjem aplikacije Entrust Entelligence i Entrust Enterprise sertifikata
5	Automatsko šifrovanje datoteka u izabranom direktorijumu korišćenjem aplikacije Entrust ICE i Entrust Enterprise sertifikata
6	Potpisivanje i šifrovanje elektronskih pisama korišćenjem Microsoft Outlook-a sa Entrust Express-om i Entrust Enterprise sertifikata
7	Importovanje Entrust Enterprise sertifikata u skladište sertifikata Microsoft Internet Explorer-a
8	Preuzimanje i instalisanje sertifikata <i>root</i> CA servera Sertifikacionog tela Pošte

9	Preuzimanje Web sertifikata
10	Potpisivanje i šifrovanje elektronskih pisama korišćenjem Microsoft Outlook-a i Web sertifikata
11	Potpisivanje i šifrovanje elektronskih pisama korišćenjem Microsoft Outlook Express-a i Web sertifikata
12	Potpisivanje Microsoft Office datoteka korišćenjem Microsoft Office aplikacija i Web sertifikata
13	Preuzimanje i instalisanje sertifikata za Web server Microsoft IIS
14	Preuzimanje i instalisanje sertifikata za Web server Apache
15	Pretraživanje, proveravanje statusa i preuzimanje sertifikata posredstvom Portala Sertifikacionog tela Pošte
16	Pretraživanje i preuzimanje sertifikata korišćenjem Address Book-a
17	Instalisanje čitača smart kartica i klijentskog softvera Datakey CIP

Literatura

- [1] "Pravilnik o elektronskim sertifikatima Javnog preduzeća PTT saobraćaja "Srbija"", "Službeni PTT glasnik", broj 341, 8.10.2004. godine (<http://www.cepp.co.yu/ca>).
- [2] Web strana Sertifikacionog tela Pošte: <http://www.cepp.co.yu/ca>.
- [3] "Ugovor o izdavanju i korišćenju elektronskog sertifikata za fizičko lice", Sertifikaciono telo Pošte (<http://www.cepp.co.yu/ca/dokumentacija>).
- [4] "Ugovor o izdavanju i korišćenju elektronskog sertifikata za pravno lice", Sertifikaciono telo Pošte.
- [5] "Preuzimanje Web sertifikata", ver. 1.1, Korisničko uputstvo, Sertifikaciono telo Pošte, 2006.
- [6] "Preuzimanje Entrust Enterprise sertifikata", ver. 1.0, Korisničko uputstvo, Sertifikaciono telo Pošte, 2004.
- [7] "Zahtev za promenu statusa elektronskog sertifikata fizičkog lica", Sertifikaciono telo Pošte.
- [8] "Zahtev za promenu statusa elektronskog sertifikata pravnog lica", Sertifikaciono telo Pošte.

Abstract: *This paper describes procedure of issuing digital certificates of the Post Serbia Certification Authority to legal and natural persons.*

Key words: *Certification Authority - CA, digital certificates, Electronic Signature Act.*

ISSUING DIGITAL CERTIFICATES OF THE POST SERBIA CERTIFICATION AUTHORITY

Dragan Spasić